

WE CLAIM

1           1. a method for authenticating validity of a public  
2   key certificate in compliance with a request, in a validation  
3   authority apparatus for certificates, said method  
4   comprising:  
5           a step of searching for paths and validating the paths  
6   searched for, beforehand;  
7           a path registration step of classifying the paths on  
8   the basis of a predetermined criterion in accordance with  
9   results of the searches and validations, and registering  
10   the classified paths in a database; and  
11          a validity authentication step of receiving the  
12   request for authenticating the validity of the public key  
13   certificate, from a terminal device, and validating the  
14   public key certificate by using the paths registered  
15   beforehand.

1           2. A method for authenticating validity of a public  
2   key certificate as defined in claim 1, wherein:  
3           in a case where, at the validity authentication step,  
4   any valid path corresponding to the validity authentication  
5   request is not registered, path search and validation are  
6   performed anew, thereby to authenticate the validity of the  
7   public key certificate.

1           3. A method for authenticating validity of a public  
2 key certificate as defined in claim 1, wherein:  
3           the predetermined criterion at the path registration  
4 step classifies the paths into valid paths and invalid paths  
5 in accordance with the results of the validations; and  
6           in a case where, at the validity authentication step,  
7 a path corresponding to the validity authentication request  
8 is registered as the valid path or the invalid path in the  
9 database, authentication of the validity of the public key  
10 certificate in the request is performed in accordance with  
11 the registered result.

1           4. A method for authenticating validity of a public  
2 key certificate as defined in claim 3, further comprising:  
3           step of performing path validation in compliance with  
4 the validity authentication request so as to check if the  
5 pertinent public key certificate and the pertinent path  
6 observe any constraint item, in a case where, at the validity  
7 authentication step, the constraint item is described in  
8 the pertinent public key certificate or any public key  
9 certificate included in the pertinent path, although the  
10 path corresponding to the validity authentication request  
11 is registered as the valid path; and  
12           step of judging the pertinent path as a valid path if  
13 the constraint item is observed.

1           5. A method for authenticating validity of a public  
2 key certificate as defined in claim 3, further comprising:  
3           step of performing path validation in compliance with  
4 the validity authentication request so as to check if the  
5 pertinent public key certificate and the pertinent path  
6 observe any policy of an electronic procedure, in a case  
7 where, at the validity authentication step, the policy is  
8 described in the validity authentication request, the  
9 pertinent public key certificate or any public key  
10 certificate included in the pertinent path, although the  
11 path corresponding to the validity authentication request  
12 is registered as the valid path; and  
13           step of judging the pertinent path as a valid path in  
14 a case where the policy is observed.

1           6. A method for authenticating validity of a public  
2 key certificate as defined in claim 3, wherein the path  
3 registration step comprises:  
4           step of searching for each path which extends from a  
5 trust anchor certificate authority to a certificate  
6 authority that issues an end entity certificate;  
7           step of acquiring and validating a certificate  
8 revocation list which concerns the end entity certificate,  
9 and which is issued by the certificate authority that issues  
10 the pertinent end entity certificate; and  
11           step of registering the certificate revocation list

12 together with a validation result thereof.

1           7. A method for authenticating validity of a public  
2 key certificate as defined in claim 6, wherein:

3           in a case where, at the validity authentication step,  
4 the path corresponding to the validity authentication  
5 request is registered as the valid path in the database,  
6 it is authenticated without validating the certificate  
7 revocation list that the pertinent public key certificate  
8 is not revoked.